Kurri, G.R., Ravi, J. y Prabhakaran, V. M. (2018). The Role of Interaction and Common Randomness in Two-User Secure Computation. In *2018 IEEE International Symposium on Information Theory (ISIT),* pp. 591-595.

DOI: https://doi.org/10.1109/ISIT.2018.8437855

The Role of Interaction and Common Randomness in Two-User Secure Computation

Gowtham R. Kurri* , Jithin Ravi† and Vinod M. Prabhakaran*
* Tata Institute of Fundamental Research, Mumbai, India. Email: k.raghunath@tifr.res.in, vinodmp@tifr.res.in
† Universidad Carlos III de Madrid, Leganés, Spain. Email: rjithin@gmail.com

***Abstract*—We consider interactive computation of randomized functions between two users with the following privacy requirement: the interactive communication should not reveal to either user any extra information about the other user's input and output other than what can be inferred from the user's own input and output. We also consider the case where privacy is required against only one of the users. For both cases, we give single-letter expressions for feasibility and optimal rates of communication. Then we discuss the role of common randomness and interaction in both privacy settings.**

I. Introduction

We consider a function computation problem between two users, Alice and Bob (Fig. 1). They observe memoryless sources (inputs) X and Y respectively and communicate interactively through a noiseless communication link to compute *randomized functions* Z_1 and Z_2 respectively. Common randomness which is independent of X and Y is available to both of them. They want to compute the functions in such a way that neither of them learn any extra information about the other user's input and output other than what its own input and output reveal. We assume that both Alice and Bob are *honest-but-curious*, i.e., they follow the given protocol, but will try to infer extra information during the protocol. Such a setup is called two-user secure computation, and it is shown in Fig. 1. The secure computation problem is specified by a pair $(q_{XY}, q_{Z_1Z_2|XY})$, where q_{XY} is the input distribution from which Alice and Bob get their inputs X and Y respectively, and $q_{Z_1Z_2|XY}$ specifies the output distribution.

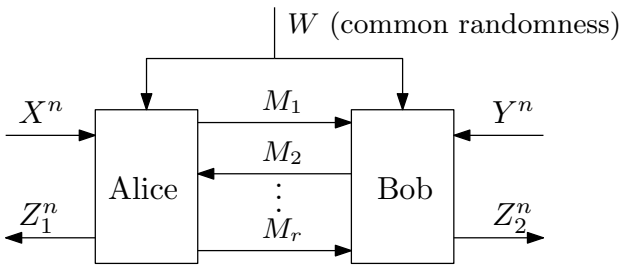

Fig. 1. Secure interactive randomized function computation. The case where Alice starts the communication is shown. Privacy against Alice requires that $M_1, \cdots, M_r$ should not reveal anything about Y^n, Z_2^n other than what can be inferred from X^n, Z_1^n. Similar conditions should hold for privacy against Bob.

Two-user interactive computation (with no privacy) has been extensively studied in computer science literature [1] as well as in information theory literature [2]–[6]. In [2], Kaspi considered two-user interactive source coding. Interactive function computation of deterministic functions was addressed in [3], [4]. The problem of computing randomized functions was studied in [5], [6].

Two-user secure computation (as described above) has been studied in cryptography under computational as well as information theoretic secrecy (see [7] and references therein). Not all functions are information theoretically securely computable by two users interacting over a noiseless link. A combinatorial characterization of securely computable deterministic functions was given in [8]. An alternative characterization using the common randomness generated by interactive communication was provided in [9]. A special case of the two-user secure computation where only Bob produces output using *a single transmission* from Alice was studied in [10], [11]. For this special case, privacy against both the users and privacy only against Alice were addressed in [10], and privacy only against Bob was considered in [11]. Single-letter expressions for optimal communication rates were obtained for these particular cases. A combinatorial characterization of two-user securely computable randomized functions is still not known, and some partial results were obtained in [12], [13]. A characterization of two-user securely computable output distributions with no inputs and no common randomness was given in [14]. In contrast to these, secrecy against an eavesdropper who has access to the interactive communication was studied in [15].

We consider our two-user secure computation problem in two privacy settings: (i) when privacy is required against both the users, (ii) when privacy is required against only one of the users. For each of these settings, we show that the set of *asymptotically* securely computable (see Definition 2) functions is the same as the that of *one-shot perfectly* securely computable functions (whose characterization still remains open as mentioned above). Further, we give single-letter expressions for the asymptotic rate regions. From the single-letter expressions we observe some interesting facts. For instance, (i) we show that for a class of functions (including deterministic functions), checking secure computability (with privacy requirement against both the users) is equivalent to checking whether cut-set bounds for computation with no privacy requirements can be met. (ii) When no privacy is required, any function can be computed in two rounds by exchanging the inputs. However, there are functions for which more rounds of interaction strictly improve the communication rate [4]. When privacy is required against both users, as was

shown in [8], if a function is securely computable, depending on the function, a certain minimum number of rounds of interaction is required for secure computation. We show that for a class of functions including deterministic functions, we can achieve any point in the rate region with this minimum number of rounds of interaction. (iii) When privacy is required against both the users, we give a necessary and sufficient condition on $(q_{XY}, q_{Z_1Z_2|XY})$ for the common randomness to be helpful in improving the communication rate.

II. Problem Formulation and Definitions

A secure randomized function computation problem is specified by a pair $\left(q_{XY}, q_{Z_1Z_2|XY}\right)$, where X, Y, Z_1 and Z_2 take values in $\mathcal{X}, \mathcal{Y}, \mathcal{Z}_1$ and $\mathcal{Z}_2$ respectively. Inputs to Alice and Bob are X^n and Y^n, respectively, where (X_i, Y_i), $i = 1, \dots n$, are independent and identically distributed (i.i.d.) with distribution q_{XY}. Both the users have access to a common random variable W, which is independent of (X^n, Y^n) and uniformly distributed over its alphabet $\mathcal{W} = [1 : 2^{nR_0}]$. The users interactively communicate in r rounds over a noiseless bidirectional link. Their goal is to *securely* compute the randomized function $q_{Z_1Z_2|XY}$, i.e., to output Z_1^n and Z_2^n, respectively, such that they are (approximately) distributed according to $q_{Z_1^nZ_2^n|X^nY^n}(z_1^n, z_2^n|x^n, y^n) := \Pi_{i=1}^n q_{Z_1Z_2|XY}(z_{1i}, z_{2i}|x_i, y_i)$ while preserving privacy in the sense that a user does not learn any additional information about the other user's input and output other than what can be inferred from the user's own input and output. We consider this problem in two different cases: (i) when privacy is required against both the users, (ii) when privacy is required against only one of the users. In both the cases we wish to determine the corresponding sets of *achievable* rates for any arbitrary $r \in \mathbb{N}$ number of rounds. Next we present the formal details of the problem statement assuming that Alice starts the communication.

Definition 1. *A* protocol Π_n *with r interactive rounds of communication consists of*

- *a set of r randomized encoders with p.m.f.'s $p^{\mathrm{E}_1}(m_i|x^n, w, m_{[1:i-1]})$ for odd numbers $i \in [1 : r]$ and $p^{\mathrm{E}_2}(m_i|y^n, w, m_{[1:i-1]})$ for even numbers $i \in [1 : r]$, where M_i is the message transmitted in the i^{th} round,*
- *two randomized decoders $p^{\mathrm{D}_1}(z_1^n|x^n, w, m_{[1:r]})$ and $p^{\mathrm{D}_2}(z_2^n|y^n, w, m_{[1:r]})$,*

Let $p^{(\text{induced})}_{X^n,Y^n,W,M_{[1:r]},Z_1^n,Z_2^n}$ denote the induced distribution of the protocol Π_n.

$$p^{(\text{induced})}(w, x^n, y^n, m_{[1:r]}, z_1^n, z_2^n) = \frac{1}{2^{nR_0}} \prod_{i=1}^{n} q(x_i, y_i) \times \left[\prod_{i:\text{odd}} p^{E_1}(m_i|x^n, w, m_{[1:i-1]}) \prod_{j:\text{even}} p^{E_2}(m_j|y^n, w, m_{[1:j-1]}) \right] \times p^{D_1}(z_1^n|x^n, w, m_{[1:r]}) p^{D_2}(z_2^n|y^n, w, m_{[1:r]}).$$

Definition 2. $(q_{XY}, q_{Z_1Z_2|XY})$ *is* asymptotically securely computable *in r rounds with privacy against both the users, if there exists a sequence of protocols Π_n, such that for every $\epsilon > 0$, there exists a large enough n such that*

$$\left\| p^{(\text{induced})}_{X^n,Y^n,Z_1^n,Z_2^n} - q_{X^n,Y^n,Z_1^n,Z_2^n} \right\|_1 \leq \epsilon, \tag{1}$$

$$I(M_{[1:r]}, W; Y^n, Z_2^n|X^n, Z_1^n) \leq n\epsilon, \tag{2}$$

$$I(M_{[1:r]}, W; X^n, Z_1^n|Y^n, Z_2^n) \leq n\epsilon, \tag{3}$$

where $q_{X^n,Y^n,Z_1^n,Z_2^n}(x^n, y^n, z_1^n, z_2^n) := \Pi_{i=1}^n \left[q_{XY}(x_i, y_i) q_{Z_1Z_2|XY}(z_{1i}, z_{2i}|x_i, y_i) \right]$.

Note that Markov chain (2) corresponds to privacy condition against Alice, which requires that Alice should not learn any additional information about Bob's input and output other than what can be inferred from her own input and output. Similarly, (3) corresponds to the privacy condition against Bob.

Definition 3. $(q_{XY}, q_{Z_1Z_2|XY})$ *is* perfectly securely computable *in r rounds with privacy against both the users, if there exists a protocol with $n = 1$ such that* (1)-(3) *are satisfied with $\epsilon = 0$.*

Definition 4. *An* (n, R_0, R_{12}, R_{21}) protocol *is a protocol* Π_n *such that the alphabet of W is $\mathcal{W} = [1 : 2^{nR_0}]$ and*

$$R_{12} = \frac{1}{n} \sum_{i:\text{odd}} \log |\mathcal{M}_i|,$$

$$R_{21} = \frac{1}{n} \sum_{i:\text{even}} \log |\mathcal{M}_i|,$$

where $\mathcal{M}_i$ is the alphabet of M_i, $i \in [1 : r]$.

Definition 5. *For a given pair $(q_{XY}, q_{Z_1Z_2|XY})$, a rate triple (R_0, R_{12}, R_{21}) is said to be* achievable *in r rounds with privacy against both the users, if there exists a sequence of (n, R_0, R_{12}, R_{21}) protocols, such that for every $\epsilon > 0$, there exists a large enough n satisfying* (1)-(3)*.*

Definition 6. *The* rate region $\mathcal{R}_A^{AB-\text{pvt}}(r)$ *(note that the subscript A denotes that Alice starts the communication) with privacy against both the users, is the closure of all the achievable rate triples (R_0, R_{12}, R_{21}).*

$\mathcal{R}_B^{AB-\text{pvt}}(r)$ can also be defined in a similar fashion for the scenario when Bob starts the communication. We are interested in the region $\mathcal{R}^{AB-\text{pvt}}(r) := \mathcal{R}_A^{AB-\text{pvt}}(r) \bigcup \mathcal{R}_B^{AB-\text{pvt}}(r)$. Let $\mathcal{R}^{AB-\text{pvt}} := \bigcup_{r=1}^{\infty} \mathcal{R}^{AB-\text{pvt}}(r)$. Notice that the above definitions are for the case when privacy is required against both the users. $\mathcal{R}_A^{A-\text{pvt}}(r)$, $\mathcal{R}_A^{B-\text{pvt}}(r)$ and so on can also be defined in a similar fashion for the cases when privacy is required only against Alice and privacy is required only against Bob, respectively. For example, for the case when privacy is required only against Alice, the definitions will require (1)-(2) only and not (3).

III. Rate Region

We present our single-letter characterizations of securely computable randomized functions and the rate regions. Proofs can be found in an extended version of this paper.

Theorem 1. *(i) $(q_{XY}, q_{Z_1Z_2|XY})$ is asymptotically securely computable in r rounds with privacy against both the users, with Alice starting the communication if and only if there exists a conditional p.m.f. $p(u_{[1:r]}|x, y, z_1, z_2)$ satisfying*

$$U_i - (U_{[1:i-1]}, X) - Y, \text{if } i \text{ is odd}, \quad (4)$$
$$U_i - (U_{[1:i-1]}, Y) - X, \text{if } i \text{ is even}, \quad (5)$$
$$Z_1 - (U_{[1:r]}, X) - (Y, Z_2), \quad (6)$$
$$Z_2 - (U_{[1:r]}, Y) - (X, Z_1), \quad (7)$$
$$U_{[1:r]} - (X, Z_1) - (Y, Z_2), \quad (8)$$
$$U_{[1:r]} - (Y, Z_2) - (X, Z_1). \quad (9)$$

(ii) $\mathcal{R}_A^{AB-\text{pvt}}(r)$ is given by the set of all non-negative rate triples (R_0, R_{12}, R_{21}) such that

$$R_{12} \geq I(X; Z_2|Y), \quad (10)$$
$$R_{21} \geq I(Y; Z_1|X), \quad (11)$$
$$R_0 + R_{12} \geq I(X; Z_2|Y) + I(U_1; Z_1, Z_2|X, Y), \quad (12)$$
$$R_0 + R_{12} + R_{21} \geq I(X; Z_2|Y) + I(Y; Z_1|X) + I(Z_1; Z_2|X, Y), \quad (13)$$

for some conditional p.m.f. $p(u_{[1:r]}|x, y, z_1, z_2)$ satisfying (4)-(9)*, $|\mathcal{U}_1| \leq |\mathcal{X}||\mathcal{Y}||\mathcal{Z}_1||\mathcal{Z}_2| + 5$ and $|\mathcal{U}_i| \leq |\mathcal{X}||\mathcal{Y}||\mathcal{Z}_1||\mathcal{Z}_2| \prod_{j=1}^{i-1} |\mathcal{U}_j| + 4, \forall i > 1$.*

Remark 1. *Part (i) of Theorem 1 implies that a pair $(q_{XY}, q_{Z_1Z_2|XY})$ is asymptotically securely computable in r rounds with privacy against both the users if and only if it is perfectly securely computable in r rounds with privacy against both the users. Note that this is similar to [10, Theorem 3]. Moreover, since the conditions do not depend on common randomness, as expected, the presence or absence of common randomness does not affect the asymptotic secure computability of a pair $(q_{XY}, q_{Z_1Z_2|XY})$.*

Remark 2. *Inequality* (12) *on $R_0 + R_{12}$ makes the rate region $\mathcal{R}_A^{AB-\text{pvt}}(r)$ asymmetric. This is in fact due to the assumption that Alice starts the communication. This is similar to the non-symmetry of the rate region observed in [5, Theorem 1].*

Our proof of part (ii) of Theorem 1 (which is omitted here) is along similar lines as [5, Theorem 1]. Constraints (10)-(13) appear in [5, Theorem 1] in a different form. The difference is because of the simplification possible here due to the additional constraints (8)-(9), which gives us (as shown in the Appendix)

$$I(X; U_{[1:r]}|Y) = I(X; Z_2|Y), \quad (14)$$
$$I(Y; U_{[1:r]}|X) = I(Y; Z_1|X), \quad (15)$$
$$I(U_{[1:r]}; Z_1, Z_2|X, Y) = I(Z_1; Z_2|X, Y). \quad (16)$$

Remark 3. *Substituting $X = Y = \emptyset$ in part (i) of Theorem 1 recovers a result of [14] which states that a distribution q_{Z_1,Z_2} is securely computable if and only if $C(Z_1; Z_2) = I(Z_1; Z_2)$, where $C(Z_1; Z_2) := \min_{Z_1 - W - Z_2} I(Z_1, Z_2; W)$ is Wyner common information [16]. To see this, note that $C(Z_1; Z_2) = I(Z_1; Z_2) + \min_{Z_1 - W - Z_2} (I(Z_1; W|Z_2) + I(Z_2; W|Z_1))$. Furthermore, when $R_0 = 0$, it can be shown using part (ii) of Theorem 1 and* (16) *that the optimal sum-rate is $R_{12} + R_{21} = C(Z_1; Z_2) = I(Z_1; Z_2)$.*

Note that Theorem 1 is for any fixed number of rounds r. The following corollary gives the region $\mathcal{R}^{AB-\text{pvt}}$. Notice that the description of region $\mathcal{R}^{AB-\text{pvt}}$ does not involve any auxiliary random variables.

Corollary 1. *If $(q_{XY}, q_{Z_1Z_2|XY})$ is asymptotically securely computable with privacy against both the users, then $\mathcal{R}^{AB-\text{pvt}}$ is given by the set of all non-negative rate triples (R_0, R_{12}, R_{21}) such that*

$$R_{12} \geq I(X; Z_2|Y), \quad (17)$$
$$R_{21} \geq I(Y; Z_1|X), \quad (18)$$
$$R_0 + R_{12} + R_{21} \geq I(X; Z_2|Y) + I(Y; Z_1|X) + I(Z_1; Z_2|X, Y). \quad (19)$$

Furthermore, suppose $r_{\min}$ is the minimum number of rounds required with either Alice or Bob starting the communication for $(q_{XY}, q_{Z_1Z_2|XY})$ to be securely computable with privacy against both the parties. Then $\mathcal{R}^{AB-\text{pvt}}(r_{\min} + 1) = \mathcal{R}^{AB-\text{pvt}}$.

For computing randomized function $(q_{XY}, q_{Z_1Z_2|XY})$ *without any privacy* guarantees, the cut-set lower bounds can be shown to be $R_{12} \geq I(X; Z_2|Y), R_{21} \geq I(Y; Z_1|X)$. The following theorem shows that for a class of functions including deterministic functions, these cut-set lower bounds for computation (without privacy) are met if and only if the function is securely computable with privacy against both the users. Let the rate region $\mathcal{R}_A^{\text{No-privacy}}(r)$ be defined along the same lines as Definition 6 (except that only correctness condition (1) is required).

Theorem 2. *Suppose the function $(q_{XY}, q_{Z_1Z_2|XY})$ is such that $H(Z_1|X, Y, Z_2) = 0$ & $H(Z_2|X, Y, Z_1) = 0$ (e.g., a deterministic function). The function is securely computable in r rounds with privacy against both the users if and only if there exists R_0 such that $\big(R_0, I(X; Z_2|Y), I(Y; Z_1|X)\big) \in \mathcal{R}_A^{\text{No-privacy}}(r)$.*

We prove this in the Appendix. The 'only if' part will follow from Theorem 1 while we show the 'if' part by showing that any protocol for computation without privacy that meets the cut-set bounds must satisfy the privacy conditions as well.

When privacy is required only against Alice, clearly, any $(q_{XY}, q_{Z_1Z_2|XY})$ is securely computable in at most 2 rounds with Alice starting the communication, as follows. Alice can transmit her input to Bob who can compute the functions according to $q_{Z_1Z_2|XY}$, and send Z_1 back to Alice. Part (i) of the following theorem considers the feasibility of 1 round protocols whereas part (ii) characterizes the rate region for an arbitrary number of rounds r.

Theorem 3. *(i) $(q_{XY}, q_{Z_1Z_2|XY})$ is asymptotically securely computable in one round with privacy only against Alice, with Alice starting the communication if and only if there exists a conditional p.m.f. $p(u_1|x, y, z_1, z_2)$ satisfying (a) $U_1 - X -$*

Y, (b) $Z_1 - (U_1, X) - (Y, Z_2)$, (c) $Z_2 - (U_1, Y) - (X, Z_1)$, (d) $U_1 - (X, Z_1) - (Y, Z_2)$.
(ii) $\mathcal{R}_A^{A-\text{pvt}}(r)$ *is given by the set of all non-negative rate triples* (R_0, R_{12}, R_{21}) *such that*

$$\begin{aligned} R_{12} &\geq I(X; U_{[1:r]}|Y), \\ R_{21} &\geq I(Y; Z_1|X), \\ R_0 + R_{12} &\geq I(X; U_{[1:r]}|Y) + I(U_1; Z_1|X, Y), \\ R_0 + R_{12} + R_{21} &\geq I(X; U_{[1:r]}|Y) + I(Y; Z_1|X) \\ &\quad + I(U_{[1:r]}; Z_1|X, Y), \end{aligned}$$

for some conditional p.m.f. $p(u_{[1:r]}|x, y, z_1, z_2)$ *satisfying* (4)-(7) *and* (8)*.*

Note that similar cardinality bounds on auxiliary random variables as in Theorem 1 and similar statements as in Remark 1 hold true for Theorem 3 also. A theorem similar to Theorem 3 holds for the case when privacy is required only against Bob and it can be found in the extended version.

IV. Role of Interaction and Common Randomness

It is clear from Remark 1 that secure computability of a pair $(q_{XY}, q_{Z_1Z_2|XY})$ does not depend on the common randomness. Discussion on the role of common randomness in this section will focus on its effect on the rate region. In [8], it was shown that for any positive integer $r \geq 2$, there exist deterministic functions Z_1 and Z_2 which require minimum r rounds of communication to securely compute Z_1 and Z_2. As in Corollary 1, we denote the minimum number of rounds required for secure computation by $r_{\min}$. It can be inferred from Corollary 1 that, when privacy is required against both the users, interaction will not help to enlarge the rate region beyond $r_{\min} + 1$ rounds. Discussion on the role of interaction below will focus on whether more number of rounds than $r_{\min}$ helps to reduce the rates.

A. Privacy required against both the users

• **For a pair $\boldsymbol{(q_{XY}, q_{Z_1Z_2|XY})}$, common randomness improves the sum rate $R_{12} + R_{21}$ if and only if $\boldsymbol{Z_1}$ and $\boldsymbol{Z_2}$ are conditionally dependent given (X, Y). Hence, for deterministic functions, common randomness does not reduce the sum rate.**

Suppose Z_1 and Z_2 are conditionally independent given (X, Y). Then due to the fact that $I(U_1; Z_1, Z_2|X, Y) \leq I(U_{[1:r]}; Z_1, Z_2|X, Y) = I(Z_1; Z_2|X, Y)$ (equality follows from (16)), (12) and (13) in Theorem 1 become redundant. Then the characterization of the rate region does not involve common randomness, which implies that common randomness is not helpful when Z_1 and Z_2 are conditionally independent given (X, Y). Now suppose Z_1 and Z_2 are conditionally dependent given (X, Y), in the absence of common randomness, the optimal sum rate $R_{12}+R_{21}$ is $I(X; Z_2|Y)+I(Y; Z_1|X)+I(Z_1; Z_2|X, Y)$ for the same reasons as above. In the presence of common randomness with rate R_0, this sum rate can be reduced to $I(X; Z_2|Y)+I(Y; Z_1|X)+\big[I(Z_1; Z_2|X, Y)-R_0\big]_+$, where $[x]_+ = \max\{x, 0\}$.

• **Interaction does not improve the sum-rate $R_{12}+R_{21}$. Interaction does not help to enlarge the rate region when i) $\boldsymbol{I(Z_1; Z_2|X, Y) = 0}$, and hence when $\boldsymbol{Z_1, Z_2}$ are deterministic functions, ii) there is large enough common randomness.**

Fix some R_0. Since $I(U_1; Z_1, Z_2|X, Y) \leq I(U_{[1:r]}; Z_1, Z_2|X, Y) = I(Z_1; Z_2|X, Y)$ (equality follows from (16)), we get from Theorem 1 that optimal sum-rate $R_{12}+R_{21}$ is $I(X; Z_2|Y)+I(Y; Z_1|X)+\big[I(Z_1; Z_2|X, Y)-R_0\big]_+$, which is the same for any number of rounds greater than or equal to $r_{\min}$. This shows that sum-rate cannot be reduced with more rounds of interaction.

When $I(Z_1; Z_2|X, Y) = 0$, due to the same reasons as mentioned above, the rate region is characterized by (10) and (11), which does not depend on auxiliary random variables and hence interaction does not enlarge the rate region.

When there is large enough common randomness, it can be observed from Theorem 1 that the rate region is again characterized by (10) and (11) and hence interaction does not enlarge the rate region.

B. Privacy required against only one user

• **Only one user computes and privacy is required against the other user: interaction and common randomness do not help to enlarge the rate region.**

Let us consider the case where only Bob computes and privacy against Alice is required. Then by substituting $Z_1 = \emptyset$ in Theorem 3, it can be observed that the only active constraint is $R_{12} \geq I(X; U_{[1:r]}|Y)$. Further, let us consider $R_{12}^* = \min I(X; U_{[1:r]}|Y)$, where the minimization is over conditional p.m.f.'s $p(u_{[1:r]}|x, y, z_2)$ satisfying (4)-(5), and

$$U_{[1:r]} - X - (Y, Z_2) \tag{20}$$

$$Z_2 - (U_{[1:r]}, Y) - X \tag{21}$$

Now let us consider $R'_{12} = \min I(X; U_{[1:r]}|Y)$ where the minimization is only under (20) and (21). Then $R_{12}^* \geq R'_{12}$. Further, it can be observed that R'_{12} is the minimum rate achievable when $r = 1$. So $R_{12}^* \leq R'_{12}$. This shows that the rate region is given by

$$\{(R_0, R_{12}, R_{21} : R_0 \geq 0, R_{12} \geq I(X; U|Y), R_{21} \geq 0\}.$$

for some conditional p.m.f. $p(u|x, y, z_2)$ satisfying $U - X - (Y, Z_2)$ and $Z_2 - (U, Y) - X$. This shows that interaction and the presence of common randomness do not help in this case.

• **One extra round from $r_{\min}$ may strictly improve the minimum sum-rate.**

We show this through an example where both the users compute a deterministic function of (X, Y), and privacy against Bob alone is required. Let Y be an m-length vector of uniform binary random variables, $Y = (Y_1, \ldots, Y_m)$, and X consists of a uniform binary random variable V and a random variable J which is uniformly distributed on $[1 : m]$, i.e., $X = (V, J)$. We assume that Y, V and J are independent. Both users want to compute function $Z = (J, V \wedge Y_J)$, where "$\wedge$" represents the binary AND function. In this example, it is easy to see that $r_{\min}$ is 2 with Bob starting the communication. We show

that the optimum sum rate $R_{12}+R_{21}$ for two round protocol is $\log m + 1/2 + m$. Then we give a three round protocol, with Alice starting the communication, which has the sum rate $\log m + 1/2 + 1$. We also show that $\log m + 1/2 + 1$ is the minimum achievable sum-rate with any r ($r \geq 3$) rounds of protocol. Details can be found in the extended version.

ACKNOWLEDGMENTS

Gowtham R. Kurri was supported by a travel fellowship from the Sarojini Damodaran Foundation. This work was done while Jithin Ravi was at Tata Institute of Fundamental Research. He has received funding from ERC grant 714161.

REFERENCES

[1] E. Kushilevitz and N. Nisan, *Communication Complexity*. New York, NY, USA: Cambridge University Press, 1997.

[2] A. Kaspi, "Two-way source coding with a fidelity criterion," *IEEE Transactions on Information Theory*, vol. 31, no. 6, pp. 735–740, Nov. 1985.

[3] A. Orlitsky and J. Roche, "Coding for computing," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 903–917, Mar. 2001.

[4] N. Ma and P. Ishwar, "Some results on distributed source coding for interactive function computation," *IEEE Transactions on Information Theory*, vol. 57, no. 9, pp. 6180–6195, Sep. 2011.

[5] M. Yassaee, A. Gohari, and M. Aref, "Channel simulation via interactive communications," *IEEE Transactions on Information Theory*, vol. 61, no. 6, pp. 2964–2982, Jun. 2015.

[6] H. Tyagi, S. B. Venkatakrishnan, P. Viswanath, and S. Watanabe, "Information complexity density and simulation of protocols," *IEEE Transactions on Information Theory*, vol. 63, no. 11, pp. 6979–7002, Nov. 2017.

[7] R. Cramer, I. Damgård, and J. Nielsen, *Secure Multiparty Computation and Secret Sharing*, 1st. New York, NY, USA: Cambridge University Press, 2015.

[8] E. Kushelvitz, "Privacy and communication complexity," *SIAM Journal on Discrete Mathematics*, vol. 5, no. 2, pp. 273–284, 1992.

[9] P. Narayan, H. Tyagi, and S. Watanabe, "Common randomness for secure computing," in *ISIT*, Jun. 2015, pp. 949–953.

[10] D. Data, "Secure computation of randomized functions," in *ISIT*, Jul. 2016, pp. 3053–3057.

[11] D. Data and V. Prabhakaran, "Secure computation of randomized functions: Further results," in *IEEE Information Theory Workshop (ITW)*, Nov. 2017, pp. 264–268.

[12] H. Maji, M. Prabhakaran, and M. Rosulek, "A unified characterization of completeness and triviality for secure function evaluation," in *INDOCRYPT*, Dec. 2012, pp. 40–59.

[13] D. Data and M. Prabhakaran, "Towards characterizing securely computable two-party randomized functions," in *Public-Key Cryptography – PKC 2018*, M. Abdalla and R. Dahab, Eds., Cham: Springer International Publishing, 2018, pp. 675–697.

[14] Y. Wang and P. Ishwar, "On unconditionally secure multi-party sampling from scratch," in *ISIT*, Jul. 2011, pp. 1782–1786.

[15] H. Tyagi, P. Narayan, and P. Gupta, "When is a function securely computable?" *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6337–6350, Oct. 2011.

[16] A. Wyner, "The common information of two dependent random variables," *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 163–179, 1975.

[17] T. Cover and J. Thomas, *Elements of Information Theory*. Wiley-Interscience, 2006.

APPENDIX

Explanation for (14)-(16)*:*

$$\begin{aligned} I(X;U_{[1:r]}|Y) &= I(X;U_{[1:r]}|Y) + I(X;Z_2|U_{[1:r]},Y) && (22)\\ &= I(X;U_{[1:r]},Z_2|Y)\\ &= I(X;Z_2|Y) + I(X;U_{[1:r]}|Z_2,Y)\\ &= I(X;Z_2|Y), && (23)\end{aligned}$$

where (22) follows from (7), and (23) follows from (9). Similarly, $I(Y;U_{[1:r]}|X) = I(Y;Z_1|X)$. Also,

$$\begin{aligned} &I(U_{[1:r]};Z_1,Z_2|X,Y)\\ &= I(U_{[1:r]};Z_1|X,Y) + I(U_{[1:r]};Z_2|X,Y,Z_1)\\ &= I(U_{[1:r]};Z_1|X,Y) && (24)\\ &= I(U_{[1:r]};Z_1|X,Y) + I(Z_2;Z_1|U_{[1:r]},X,Y) && (25)\\ &= I(U_{[1:r]},Z_2;Z_1|X,Y)\\ &= I(Z_1;Z_2|X,Y) + I(U_{[1:r]};Z_1|Z_2,X,Y)\\ &= I(Z_1;Z_2|X,Y), && (26)\end{aligned}$$

where (24) follows from (8), (25) follows from (7), and (26) follows from (9).

Proof of Theorem 2*:* 'Only if' direction follows directly from Theorem 1. For the 'if' direction, we show that if a scheme computes $(q_{XY}, q_{Z_1Z_2|XY})$ with R_{12} and R_{21} equal to $I(Z_2;X|Y)+\delta$ and $I(Z_1;Y|X)+\delta$ respectively, and with some R_0, under no privacy, then this scheme will also satisfy the privacy conditions (2)-(3). From the converse of [5, Theorem 1], we have $nR_{12} \geq I(M_{[1:r]};X^n|Y^n,W)$. Then we get

$$\begin{aligned} nR_{12} &\geq I(M_{[1:r]};X^n|Y^n,W)\\ &= I(M_{[1:r]},W;X^n|Y^n) && (27)\\ &= I(M_{[1:r]},W;X^n|Y^n)\\ &\quad + I(Z_2^n;X^n|M_{[1:r]},W,Y^n) && (28)\\ &= I(Z_2^n,M_{[1:r]},W;X^n|Y^n)\\ &= I(Z_2^n;X^n|Y^n) + I(M_{[1:r]},W;X^n|Y^n,Z_2^n)\\ &= I(Z_2^n;X^n|Y^n) + I(M_{[1:r]},W;X^n,Z_1^n|Y^n,Z_2^n)\\ &\quad - I(M_{[1:r]},W;Z_1^n|X^n,Y^n,Z_2^n)\\ &\geq I(Z_2^n;X^n|Y^n) + I(M_{[1:r]},W;X^n,Z_1^n|Y^n,Z_2^n)\\ &\quad - H(Z_1^n|X^n,Y^n,Z_2^n)\\ &\geq n\left[I(Z_2;X|Y) - \epsilon_1\right] + I(M_{[1:r]},W;X^n,Z_1^n|Y^n,Z_2^n)\\ &\quad - n\left[H(Z_1|X,Y,Z_2) + \epsilon_2\right], && (29)\end{aligned}$$

where (27) is due to the independence of common randomness W and (X^n,Y^n), (28) follows from the Markov chain $Z_2^n - (W,Y^n,M_{[1:r]}) - (X^n,Z_1^n)$. We used the following fact in (29): if two random variables A and A' with same support set $\mathcal{A}$ satisfy $||p_A - p_{A'}||_1 \leq \epsilon \leq 1/4$, then it follows from [17, Theorem 17.3.3] that $|H(A) - H(A')| \leq \eta \log|\mathcal{A}|$, where $\eta \to 0$ as $\epsilon \to 0$. Now (1) implies (29), where $\epsilon_1, \epsilon_2 \to 0$ as $\epsilon \to 0$. When $H(Z_1|X,Y,Z_2) = 0$, from (29) we have $I(M_{[1:r]},W;X^n,Z_1^n|Y^n,Z_2^n) \leq \delta + \epsilon_1 + \epsilon_2$ for $\delta \to 0$, and $\epsilon_1, \epsilon_2 \to 0$ as $\epsilon \to 0$, which is the required privacy condition against Bob. Similar argument holds for R_{21} when $H(Z_2|X,Y,Z_1) = 0$. ■